**Chapter 19 Questions**

**Q19-1.**Can the value of the header length field in an IPv4 packet be less than 5?   
When is it exactly 5?

Ans: The min length of the IPv4 header is 20 bytes and the maximum length of the IPv4 header is 60 bytes. The value of the header length field defines the header length in multiples of four bytes, which means that HLEN can be between 5 and 15. It cannot be less than 5 and it cannot be greater than 15. It is exactly 5 when there is no option.

**Q19-2.**A host is sending 100 datagrams to another host. If the identification number of the first datagram is 1024, what is the identification number of the last?

Ans: The identification numbers need to be contiguous. The identification number of the last datagram should be 1024 + 100 − 1 = 1123.

**Q19-3.**An IP fragment has arrived with an offset value of 100. How many bytes of data were originally sent by the source before the data in this fragment?

Ans: An offset of 100 indicates that the first byte in this fragment is numbered 800, which means bytes numbered 0 to 799 (for a total of 800 bytes) were sent before.

**Q19-4.**Mention the three auxiliary protocols at the network layer of the TCP/IP suite that are designed to help the IPv4 protocol.

Ans: The three auxiliary protocols are ICMP, IGMP, and ARP.

**Q19-5.**In an IPv4 datagram, the value of the header-length (HLEN) field is (6)16. How many bytes of options have been added to the packet?

Ans: The header length is 6 ⋅ 4 = 24. The option length is then 24 − 20 = 4 bytes.

**Q19-6.**Can each of the following be the value of the TTL in a datagram? Explain your answer.

Ans: **a.** 23 Yes. The TTL field is 8 bits, which means that the maximum value of TTL is 255 bits. **b.** 0 No, Datagram is discarded when TTL is 0 also because it means that the packet cannot travel at all. **c.** 1 Yes. This would the last hop of the datagram. **d.** 301 No, because the length of the value field id 8 bits which means the max value is 255.

**Q19-7.**Compare and contrast the protocol field at the network layer with the port numbers at the transport layer. What is their common purpose? Why do we need two port-number fields but only one protocol field? Why is the size of the protocol field only half the size of each port number?

Ans: The protocol field and the port numbers both have the same functionality i.e **Multiplexing** and **Demultiplexing**. Port numbers are used to do these tasks at the transport layer. But the protocol field is used to do the same at the network layer. We need only one protocol field at the network layer because payload taken from a protocol at the source should be delivered to the same protocol at the destination. The client and server processes, on the other hand, normally have different port numbers (ephemeral and well-known), which means we need two port numbers to define the processes. The size of the protocol field defines the total number of different protocols that use the service of the net- work layer, which is a small number (eight bits is enough for this purpose). On the other hand, many new applications may by added every day that needs a larger size of the port number field (sixteen bits is assigned).

**Q19-8.**Which field(s) in the datagram is(are) responsible for gluing together all fragments belonging to an original datagram?

Ans: Two fields, source IP address and the identification, are needed to uniquely define fragments belonging to the same datagram. The value of the identification field is not enough because two sources may start with the same identification number.

**Q19-9.**Can each of the following be the value of the offset field in a datagram? Explain your answer.

Ans: **a.** 8 - Yes, Fragments are specified in units of 8 bytes, which is why fragment length must be a multiple of 8, so it can be used as offset value for next packet.

**b.** 31 No, Fragments are specified in units of 8 bytes, which is why fragment length must be a multiple of 8, and it cannot be used as offset value for next packet.

**c.** 73 - No, Fragments are specified in units of 8 bytes, which is why fragment length must be a multiple of 8 and it cannot be used as offset value for next packet.

**d.** 56 , Yes, Fragments are specified in units of 8 bytes, which is why fragment length must be a multiple of 8, so it can be used as offset value for next packet.

**Q19-10.**Assume a destination computer receives several packets from a source. How can it be sure that the fragments belonging to a datagram are not mixed with the fragments belonging to another datagram?

Ans: Each datagram should have a unique identification number that distinguishes it from other datagrams sent by the same source. The identification number is copied into all fragments. In other words, the identification number glues all fragments belonging to the same datagram together.

**Chapter 19 Problems**

**P19-1.**In an IPv4 datagram, the value of total-length field is (00A0)16 and the value of the header-length (HLEN) is (5)16. How many bytes of payload are being carried by the datagram? What is the efficiency (ratio of the payload length to the total length) of this datagram?

Solution: The total length of the datagram is (00A0)16 = 160 bytes. The header length is 5 ⋅ 4 = 20. The size of the payload is then 160 − 20 = 140. The efficiency = 140 / 160 = 87.5%.

**P19-2.**An IP datagram has arrived with the following partial information in the header (in hexadecimal): **45000054 00030000 2006...**

**a.What is the header size?**

**Ans:** The second hex digit in the first byte is 5 (HLEN), which means that the   
header length is only 5 × 4 = 20 bytes.

**b.Are there any options in the packet?**

**Ans:** There are no options because the header size is only 20 bytes.

**c.What is the size of the data?**

**Ans:** The total length of the packet is (0054)16 or 84 bytes. Since the header is 20 bytes, it means the packet is carrying 64 bytes of data.

**d.Is the packet fragmented?**

**Ans:** Since the flags field fragmentation offset bit is all 0s, the packet is not fragmented.

**e.How many more routers can the packet travel to?**

**Ans:** The value of the TTL field is (20)16 or 32 in decimal, which means the packet may visit up to 32 more routers.

**f. What is the protocol number of the payload being carried by the packet?**

**Ans:** The value of the protocol field is 6, which means that the packet is carrying a segment from the TCP protocol.

**23 Questions**

**Q23-1.**Assume we have a set of dedicated computers in a system, each designed to perform only a single task. Do we still need host-to-host and process-to- process communication and two levels of addressing?

Ans: No. Host-to-host and process-to-process communication are needed because each computer in the Internet is designed to do multiple tasks: to run multiple application-layer programs.

**Q23-2.**Operating systems assign a process number to every running application pro- gram. Can you explain why these process numbers cannot be used instead of port numbers?

Ans: When a server process starts running on the server, its number should be advertised by the server to all possible clients that need to contact that process. This can be done for client processes, it is very inefficient, if not impossible, for the server processes.

**Q23-3.**Assume you need to write and test a client-server application program on two hosts you have at home.

1. What is the range of port numbers you would choose for the client program?

Ans: 49,152 to 65,535.

**b.** What is the range of port numbers you would choose for the server program?

Ans: 49,152 to 65,535.

**c.** Can the two port numbers be the same?

Ans: Yes but it is advisable to choose different port numbers for the server and the client to be able to better debug the programs.

**Q23-4.**Assume a new organization needs to create a new server process and allow its customers to access the organization site using that process. How should the port number for the server process be selected?

Ans: The organization needs to select a port number from the registered range, 1024 to 49,151, and register that port number with ICANN. If the port number is already in use, ICANN informs the organization to choose another port number in this range.

**Q23-5.**In a network, the size of the receive window is 1 packet. Which of the follow- ing protocols is being used by the network?

**a.** Stop-and-Wait - Yes

**b.** Go-Back-*N -* No

**c.** Selective-Repeat - No

**Q23-6.**In a network, the size of the send window is 20 packets. Which of the follow- ing protocols is being used by the network?

1. Stop-and-Wait - No
2. **b.** Go-Back-*N -* Yes
3. **c.** Selective-Repeat - Yes

**Q23-7.**In a network with fixed value for *m* > 1, we can either use the Go-Back-*N* or the Selective-Repeat protocol. Describe the advantage and the disadvantage of using each. What other network criteria should be considered to select either of these protocols?

Ans:

a. The advantage of using the Go-Back-N protocol is that we can have a larger send window size. We can send more packets before waiting for their acknowledgment. The disadvantage of using this protocol is that the receive window size is only 1. The receiver cannot accept and store the out- of-order received packets; they will be discarded. Discarding of the out-of- order packets means resending these packets by the sender, resulting in congestion of the network and reducing the capacity of the pipe. So the advantage seen by a larger send window may disappear by filling the net- work with resent packets.

b. The advantage of using the Selective-Repeat protocol is that the receive window can be much larger than 1. This allows the receive window to store the out-of-order packets and avoids resending them to congest the network. The disadvantage of this protocol is that the send window size is half of the Go-Back-N, which means that we can send fewer packets before waiting for the acknowledgment.

We can conclude that if the bandwidth-delay product of the network is large, the reliability is good, and the delay is low, we should choose the Go-Back-N protocol to use more of the network capacity. On the other hand, if the band- width-delay product is small, or the network is not very reliable, or the net- work creates long delays, we need to use Selective-Repeat.

**Q23-8.**Since the field that stores the sequence number of a packet is limited in size, the sequence number in a protocol needs to wrap around, which means that two packets may have the same sequence number. In a protocol that uses *m* bits for the sequence-number field, if a packet has the sequence number *x*, how many packets need to be sent to see a packet with the same sequence number *x*, assuming that each packet is assigned one sequence number?

Ans: Sequence numbers use modulo 2m arithmetic. This means that if a packet has the sequence number x, 2m packets need to be passed to see the same sequence number if each packet uses only one sequence number (not in TCP, where the sequence number defines the number of the first byte in the packet).

**Q23-9.**Does the wraparound situation we discussed in the previous question create a problem in a network?

Ans: The networks need to be carefully designed to make the time between the two wraparounds as long as possible. For example, in a protocol that uses the sequence number field of size 3 (m = 3), every 2m = 8 packets have the same sequence number. If the previous packet with sequence number x (or its accidentally created duplicate) is still wandering in the network arrives at the destination, the receiver may confuse this with the expected new packet, also with sequence number x.

**Q23-10.**Can you explain why some transport-layer packets may be received out of order in the Internet?

Ans: The transport-layer packets are encapsulated in the datagram at the network layer. Each IP packet may travel a different route and arrives at the destination with a different delay. If a packet encounters more delay than the next packet, it will be received out of order.

**Q23-11.**Can you explain why some transport-layer packets may be lost in the Internet?

Ans: The transport-layer packets are encapsulated in the datagram at the network layer. The router through which the datagrams need to pass to reach their destination may be congested and drop the packets.

**Q23-12.**Can you explain why some transport-layer packets may be duplicated in the   
Internet?

Ans: If a transport layer protocol such as TCP uses a timer and resends some packets that have not arrived at the destination on time, it may happen that both the original and the resent packet arrive at the destination.

**Q23-13.**In the Go-Back-*N* protocol, the size of the send window can be 2*m* − 1, while   
the size of the receive window is only 1. How can flow control be accomplished when there is a big difference between the size of the send and receive windows?

Ans: The rest of the packets (2m − 2) are supposed to be in transit, filling the pipe. The size of the receive window is chosen to be 1 to accept only one packet, the one expected, and not out-of order packets. The receiver cannot be over- whelmed because it holds only one packet in its window. When the only packet in the window is consumed by the upper-layer protocol, the receive window slides to make it possible to receive the next packet in transit. If any packet in transit arrives before the window slides, it is discarded.

**Q23-14.**In the Selective-Repeat protocol, the size of the send and receive windows is the same. Does this mean that there are supposed to be no packets in transit?

Ans: There can be several packets still in transit. The size of the receive window is chosen to be the same as the size of the send window to accommodate out-of- order packets until a set of packets all in order arrives. The protocol does not want to deliver the out-of-order packets to the application-layer protocol.

**23.4.3 Problems**

**P23-1.**Compare the range of 16-bit addresses, 0 to 65,535, with the range of 32-bit IP addresses, 0 to 4,294,967,295 (discussed in Chapter 18). Why do we need such a large range of IP addresses, but only a relatively small range of port numbers?

Solution: IP stands for Internet Protocol Address. It is an addressing scheme used to identify system on the network. It is the unique identification given to host, network device and server for the communication. A 16 bit IP address is the number represented in two decimal numbers where each decimal number is of 8 bits. The range of 16 bit addresses is 0 to 65,535. 32 bit IP addressing is the number represented in 4 decimal numbers where each decimal number is of 8 bits. NEED FOR LARGE RANGE OF IP ADDRESSES. The main reason the limited number of addresses.

* The rapid exhaustion of IPv4 address space prompted to explore new technologies to expand the addressing capacity in the internet. If the range of IP address is increased then it is deemed sufficient for the foreseeable future. More address space is required to connect new devices in the future. So large range of IP addresses are used.
* PORT Numbers. The range of port numbers is small because if we have large range of port numbers in praise then they can be exhausted.
* The domain of IP addresses is universal. A device directly connected to the Internet needs a unique IP address. The domain of port numbers is local; they can be repeated. Two computers running the HTTP server process use the same well-known port number (80); two computers running the HTTP client process can use the same ephemeral port number.

**P23-2.**Can you explain why ICANN has divided the port numbers into three groups: well-known, registered, and dynamic?

Solution: Since port numbers have local jurisdiction and can be repeated, the division distinguishes between client processes and server processes to avoid confusion when a host runs client and server processes at the same time. For example, assume host A is running a client process with the port number x, which has sent out a request and is waiting for a response from the corresponding server. Host B sends a request to a server process with the port number x, which is received by host A. Host A erroneously passes the request to the cli- ent process with port number x, assuming that this is the response that the client process is waiting for. If client and server were using different port numbers, x and y for example, the request received by host A would be dropped because no server with port number y was running. ICANN has also divided the server port numbers into two groups. The well-known port numbers are recognized through the whole Internet society; the registered port numbers are those that do not have a universal jurisdiction yet.

**P23-3.**A sender sends a series of packets to the same destination using 5-bit sequence numbers. If the sequence numbers start with 0, what is the sequence number of the 100th packet?

Solution: The sequence number of any packet can be found using the following relation:

seqNo = (starting segNo + packet number −1) mod 2m   
in which m is the number of bits used to define the sequence number.

The sequence number in this case is   
seqNo= (0+100−1)mod25 = 99mod32= 3

**P23-4.**In each of the following protocols, how many packets can have independent sequence numbers before wraparound occurs (see the previous problems).  
**a.** Stop-and-Wait, *m* = 1, every 2m = 2 packets have the same sequence number.   
**b.** Go-Back-*N* with *m* = 8, every 2m = 256 packets have the same sequence number.   
**c.** Select-Repeat with *m* = 8, every 2m = 256 packets have the same sequence number.

**P23-5.**Using 5-bit sequence numbers, what is the maximum size of the send and   
receive windows for each of the following protocols?

1. Stop-and-Wait - 1 for the send window and 1 for receive window.   
   **b.** Go-Back-*N -* 2 *raise to power* 5 - 1 = 31 for the send and 1 for receive.  
   **c.** Selective-Repeat - 2 *raise to power* 5 / 2 = 16 for both send and receive window.